

CLAIMS

1 1. (previously presented) A unitary portable biometrics-based access control
2 device which can be directly plugged into a universal serial bus (USB) socket
3 communicatively coupled to a restricted resource, the device comprising:
4 a housing;
5 a microprocessor housed within the housing;
6 a USB plug integrated into the housing without an intervening cable and capable of
7 coupling the unitary portable access control device directly to the USB socket; and
8 a biometrics-based authentication module coupled to and controlled by the
9 microprocessor, at least a portion of the biometrics-based authentication module being
10 housed within the housing, wherein access to the restricted resource is granted to a user
11 provided that the biometrics-based authentication module authenticates the user's identity and
12 wherein access to the restricted resource is denied to the user otherwise.

1 2. (previously presented) The portable device as recited in Claim 1 wherein the
2 biometrics-based authentication module is a fingerprint authentication module.

1 3. (previously presented) The portable device as recited in Claim 1 wherein the
2 biometrics-based authentication module is an iris scan authentication module.

1 4. (previously presented) The portable device as recited in Claim 1 wherein the
2 biometrics-based authentication module comprises a biometrics sensor fitted on one surface
3 of the housing.

1 5. (previously presented) The portable device as recited in Claim 1 further
2 comprising a non-volatile memory capable of storing biometrics information usable for
3 authentication.

1 6. (previously presented) The portable device as recited in Claim 1 wherein the
2 microprocessor is configured to provide a bypass mechanism for authentication upon a
3 determination of authentication failure by the biometrics-based authentication module.

1 7. (previously presented) The portable device as recited in Claim 1 wherein the
2 restricted resource comprises a host computer.

1 8. (previously presented) The portable device as recited in Claim 1 wherein the
2 restricted resource comprises a communication network.

1 9. (previously presented) The portable device as recited in Claim 1 wherein the
2 restricted resource is a real estate premises that imposes access restrictions.

1 10. (previously presented) The portable device as recited in Claim 1 wherein the
2 restricted resource is an operable machinery, the safe operation of which requires training.

1 11. (previously presented) A biometrics-based access control system for
2 controlling access to a restricted resource, comprising:
3 a portable device which can be directly plugged into a universal serial bus (USB)
4 socket communicatively coupled to the restricted resource and which includes a housing; a
5 non-volatile memory housed within the housing; a USB plug integrated into the housing
6 without an intervening cable and capable of coupling the portable device directly to the USB
7 socket; and a biometrics-based authentication module coupled to the non-volatile memory,
8 wherein the biometrics-based authentication module is configured to (1) capture a first
9 biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3)
10 capture a second biometrics marker; and (4) determine whether the second biometrics marker
11 can be authenticated against the first biometrics marker, and wherein access to the restricted
12 resource is granted upon a determination of successful authentication and wherein access to
13 the restricted resource is denied otherwise.

1 12. (previously presented) The biometrics-based access control system as recited
2 in Claim 11 wherein the biometrics-based authentication module is a fingerprint
3 authentication module.

1 13. (previously presented) The biometrics-based access control system as recited
2 in Claim 11 wherein the biometrics-based authentication module is an iris scan authentication
3 module.

1 14. (previously presented) The biometrics-based access control system as recited
2 in Claim 11 wherein the biometrics-based authentication module comprises a biometrics
3 sensor which is structurally integrated with the portable device in a unitary construction, the
4 biometrics sensor being disposed on one surface of the housing of the portable device.

1 15. (previously presented) The biometrics-based access control system as recited
2 in Claim 11 wherein the non-volatile memory of the portable device comprises flash memory.

1 16. (previously presented) The biometrics-based access control system as recited
2 in Claim 11 wherein a bypass mechanism for authentication is provided upon a determination
3 of authentication failure by the biometrics-based authentication module.

1 17. (previously presented) A biometrics-based access control method for
2 controlling access to a restricted resource and implemented using a portable device, the
3 method comprising the steps of:

4 (a) directly plugging the portable device into a universal serial bus (USB) socket
5 communicatively coupled to the restricted resource, wherein the portable device includes a
6 housing; a memory; a biometrics sensor; and a USB plug integrated into the housing without
7 an intervening cable and capable of coupling the portable device directly to the USB socket;

8 (b) obtaining a first biometrics marker from a user with the biometrics sensor of
9 the portable device;

10 (c) retrieving a registered biometrics marker from the memory of the portable
11 device, the registered biometrics marker having been stored therein during a registration
12 process;

13 (d) comparing the first biometrics marker against the registered biometrics
14 marker; and

15 (e) granting the user access to the restricted resource provided that a match is
16 identified in said step (d).

1 18. (previously presented) The biometrics-based access control method as recited
2 in Claim 17 wherein the registered biometrics marker is a fingerprint.

1 19. (previously presented) The biometrics-based access control method as recited
2 in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

1 20. (previously presented) The biometrics-based access control method as recited
2 in Claim 17 further comprising the step of denying the user access to the restricted resource
3 provided that a match is not identified in said step (d).

1 21. (previously presented) The biometrics-based access control method as recited
2 in Claim 17 further comprising the step of providing the user with a bypass authentication
3 procedure provided that a match is not identified in said step (d).